To: Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W., Suite TW-A325
Washington, DC 20554

Unified Office, Inc.
20 Trafalgar Square
Nashua, NH 03063
Annual 47 C.F.R. 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009 (e) CPNI Certification for 2016 covering the calendar year ended December 31, 2016.

Date filed: September 19, 2017

This Certification applies to Unified Office, Inc. ("Unified Office" or "the Company")

Name of signatory: Peter White

Title of signatory: Chief Financial Officer of Unified Office, Inc.

Certification:

I, Peter White, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The Company has not received customer complaints in the past year concerning the unauthorized release of CPNI in the past year.

Signed: Peter White

ACCOMPANYING STATEMENT EXPLAINING CPNI PROCEDURES
SUMMARY OF CUSTOMER COMPLAINTS

This statement accompanies the Company's Customer Proprietary Network Information ("CPNI") Certification for the year ended December 31, 2016, as required by Section 64.2009 (e) of the Federal Communications Commission's ("FCC") rules, for the purpose of explaining how the operating procedures of the Company ensure compliance with part 64, Subpart U of the FCC's rules. See 47 C.F.R. 64.2001 *et seq.* The below procedures are specifically designed to comply with the Commission's CPNI rules and regulations, as well as to maintain the security of the CPNI of the Company's customers.

All subsequent references to rule Sections refer to rules under Part 64, Subpart U unless indicated otherwise.

1. Operating Procedures

Changes to Account Information

Pursuant to Section 64.2010 (f), when a customer's account information or password has been modified, the Company immediately sends a text notification to the customer's phone number notifying him or her that a change has been made to the account, and that the customer should call customer service with any questions. If such customer is unable to receive a text message or, if the Company receives a reply that the message could not be delivered, the Company mails a letter to the customer's address of record.

Customer Initiated Calls

Customer service representatives are trained that in order to discuss call details or other CPNI during a customer initiated phone call, customers must first be properly authenticated by proving a password meeting the requirements of Section 64.2010 (b). In the event a customer forgets his/her password, the Company has implemented password back-up authentication procedures in compliance with Section 64.2010 (e).

2. Training Procedures

The Company has established procedures to train employees having access to, or occasion to use customer data. Employees are trained to identify CPNI, consistent with the definition of CPNI under Section 64.2003 (g) and Section 222 (F) (1) of the Communications Act of 1934 as amended (47 U.S.C. 222 (f) (1). Likewise, employees are trained on safeguards to protect CPNI and as to when they are and are not authorized to use CPNI. Training occurs at the time of hire and again as required.

In addition, the IT department periodically updates the Company's CPNI Protection Policy, which every employee must read and sign. All employees have access to CPNI resources and guidelines in the event they have additional questions about CPNI and CPNI related issues.

3. Supervisory Review

At this time, the Company does not use CPNI for outbound marketing purposes that requires either opt-out or opt-in consent. Before taking to use CPNI for outbound marketing purposes that require such consent, the Company will establish review procedures to ensure compliance with Section 64.2009 (d).

4. Customer Notification and Authorization Process

The Company does not currently use CPNI for marketing purposes that require either opt-out or opt-in consent in accordance with the Commission's rules. Prior to initiation of any program for the use of CPNI for marketing purposes, except as allowed under the Commission's rules, the Company will train employees with a need and/or responsibility for obtaining customer authorization to use CPNI for marketing purposes, regarding the notice and approval requirements under Section 64.2008.

5. Recordkeeping of Use of CPNI

As mentioned above, the Company currently does not utilize an opt-out or opt-in consent process. At such time as the Company may initiate use of CPNI for marketing, the Company will develop and utilize a system for maintaining readily accessible records.

6. Disciplinary Process

The Company has in place an express disciplinary process to address any unauthorized use of or access to CPNI. Employees are notified that any infraction involving CPNI will result in disciplinary action up to and including termination of employment.

7. Procedures for Notifying Law Enforcement of CPNI Security Breaches

The Company has adopted procedures to comply with Section 64.2011 for notifying law enforcement of CPNI security breaches, together with related recordkeeping and deferred notification to customers. If an incident or customer complaint appears to involve CPNI, a designated CPNI manager within the Company is notified. The CPNI manager will analyze the situation, maintain a detailed report and inform law enforcement if necessary pursuant to 64.2011. The manager also maintains records o incidents pursuant to Section 64.2011 (d).

8. Actions Taken Against Data Brokers and Responses to Customer Complaints

No actions were taken against data brokers in 2015.

The Company received no customer complaints concerning the unauthorized release of CPNI in 2016.

CPNI Template Submission

Customer Proprietary Network Information (CPNI) Certification Home

Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template
EB Docket 06-36

This web page allows you to file your annual Customer Proprietary Network Information (CPNI) certification statements electronically. Complete the following fields, and make sure you have access to all the supporting file attachments you wish to submit before continuing to step 2.

Annual 64.2009(e) CPNI Certification for 2017 covering the prior calendar year 2016

1. Date filed: 9/20/2017

2. Name of company(s) covered by this certification: [Company Names will be automatically populated when you proceed to Step 2 of this process based on Form 499-A Filer ID(s) entered below.]

3. Form 499 Filer ID(s): 831695

4. Name of signatory: Peter White

5. Title of signatory: Chief Financial Officer

6. Certification:

I, Peter White [name of officer signing certification] , certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those

mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company [○ has ◉ has not] taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. [NOTE: If you reply in the affirmative, please provide an explanation of any actions taken against data brokers.]

The company [○ has ◉ has not] received customer complaints in the past year concerning the unauthorized release of CPNI [NOTE: If you reply in the affirmative, please provide a summary of such complaints. This summary should include number of complaints, broken down by category or complaint, *e.g.,* instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.]

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed: [☑ Signature of an officer, as agent of the carrier] Peter White

Proceed to Step 2: Upload File Attachments

Return to CPNI Home

Federal Communications Commission
445 12th Street SW
Washington, DC 20554
More FCC Contact Information...

Phone: 1-888-CALL-FCC (1-888-225-5322)
TTY: 1-888-TELL-FCC (1-888-835-5322)
Fax: 1-866-418-0232
E-mail: fccinfo@fcc.gov

CPNI Template Submission Software Version 00.01.03 April 5, 2011

Unified Office Customer Private Network Information (CPNI) Protection Policy

Introduction

In the course of providing the Total Connect Now service, Unified Office collects information about its customer's configurations and usage of the service. That information includes: (1) information about the quantity, technical configuration, type, destination, location, and amount of use of the service, (2) information contained on bills concerning the service. That information, when matched to a name, address, and telephone number is known as "Customer Proprietary Network Information," (CPNI).

Federal law requires that the confidentiality of this information is protected. This document details the processes and procedures that Unified Office uses to protect CPNI.

Access to CPNI

There are several classes of people who may have access to CPNI and protections to ensure proper access:

Unified Office Employees and Contractors (UO staff) — UO staff have access to CPNI as necessary in the performance of their jobs. Access is via passwords that can be revoked in case the staff member departs the company. Strict adherence to passwords is required. Firewalls are in place.

UO staff may have access to call details and/or recorded calls. These calls details and recordings will only be provided to an authorized party representing the customer, whose identity will be confirmed and authenticated prior to dissemination of recorded calls.

The Company has established procedures to train employees having access to, or occasion to use customer data. Employees are trained to identify CPNI. Employees are trained on safeguards to protect CPNI and as to when they are and are not authorized to use CPNI. Training occurs at the time of hire and again as required. Employees acknowledge in writing their compliance with the Company CPNI policy.

Unified Office Resellers (Resellers) — Resellers are independent agents who are responsible for supporting subsets of the Unified Office customers. They have access to some CPNI for their customers (only) via a variety of websites. All website access is controlled through individual usernames and passwords. Passwords must conform to complexity requirements such as minimum length and variety of characters. UO staff creates an initial website account for a designated reseller representative. This account is usually assigned the privilege of creating additional accounts with access to the data of the reseller's customers. These additional accounts may contain restrictions on the scope of data visible to the user

Screened
FCC C
SEP 26

Customers — Customers have access to CPNI through a variety of websites. All website access is controlled through individual usernames and passwords. Passwords must conform to complexity requirements such as minimum length and variety of characters. For a given customer, UO staff creates an initial website account for a designated customer representative. This account is usually assigned the privilege of creating additional accounts with access to the customer's data. These additional accounts may contain restrictions on the scope of data visible to the user.

When a customer's account information or password has been modified, the Company immediately sends notification to the customer notifying him or her that a change has been made to the account. If such customer is unable to receive the message or if the Company receives a reply that the message could not be delivered, the Company mails a letter to the customer's address of record.

Law Enforcement — Unified Office will disclose CPNI to law enforcement agents in possession of legal warrants detailing the information that must be disclosed.

Breach of CPNI Privacy

In the event Unified Office experiences a privacy breach and CPNI is disclosed to unauthorized persons, federal rules require Unified Office to report such breaches to law enforcement. Specifically, Unified Office will notify law enforcement no later than seven (7) business days after a reasonable determination that such a breach has occurred by sending electronic notification through a central reporting facility to the United States Secret Service and the FBI. Unified Office will inform affected customers of the breach as soon as allowed to by law enforcement. As required by federal law, Unified Office will maintain records of each discovered breach, include the date of discovery, the date and contents of the notification sent to law enforcement, a detailed description of the breach and law enforcement's response. Unified Office will retain these records for a period of not less than two years.